ECE803 Coursework

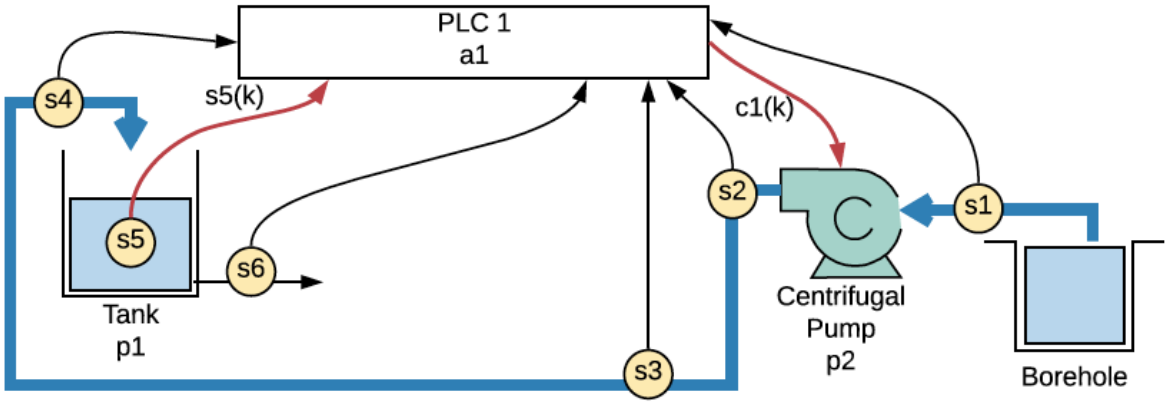
Friday, 13 November (Hand-in Friday 27 November)

Question 1

Considering Electricity, Communications and Health sectors in Cyprus, sketch a dependency diagram showing how these inter-relate. Construct a narrative, possibly using a ripple diagram, about how a failure in communications affects the other two services – consider the first few minutes and then the effect of a blackout for a day and then a week.

Question 2

Consider a simplified version of the water distribution example from Part 2 of the notes:



Part a. Some of the sensors are redundant in this picture but the PLC needs to detect low level in the tank and the presence of water at s1 and has the ability to start the pump. The sensors s1 and s2 are pressure sensors, s3, s4 and s6 are flow sensors and s5 is a level sensor. The parameter to s5 is a level reading and should be ignored for this exercise – instead treat s5 as a Boolean representing sufficient or insufficient water in the tank. Similarly, the parameter to c1 can be ignored and it can be treated as a Boolean that starts or stops the pump. Focussing mainly on s1, s5 and the pump, sketch part of the ladder logic for the PLC.

Part b. Describe two ways in which an attacker might seek to disrupt the operation of this system.

Part c. Suppose that the PLC is a MicroLogix 1100 with the vulnerabilityCVE-2016-0868 unpatched. Considering the two stage kill chain, sketch how an attacker might exploit this. You might find it helpful to read the appropriate advisory from ICS-CERT and consider the correlated attacks from the course notes.

Part d. Suggest some mitigations to prevent your chosen attack.